**Incident handler's journal**

|  |  |
| --- | --- |
| **Date:**  Feb 29, 2023 | **Entry:** #1 |
| Description | Documenting a cybersecurity incident  Two phases:   1. **Detection and Analysis**: The description outlines how the organization first detected the ransomware incident. For the analysis step, the organization contacted several organizations for technical assistance. 2. **Containment, Eradication, and Recovery**: The scenario details some steps that the organization took to contain the incident. For example, the company shut down their computer systems. However, since they could not work to eradicate and recover from the incident alone, they contacted several other organizations for assistance. |
| Tool(s) used | None. |
| The 5 W's | * **Who**: An organized group of unethical hackers * **What**: A ransomware security incident * **When**: Tuesday 9:00 a.m. * **Where**: At a health care company * **Why**: This incident occurred because an unethical hacker used a phishing attack to gain access to the company's systems. After gaining access, the attacker ran ransomware on the company's systems to encrypt important files. The attackers appear to have been motivated financially, as they used the ransom money they left behind to demand a large amount of money in return for the decryption key. |
| Additional notes | 1. How could the company prevent an incident like this from occurring again? 2. Should the company pay for the ransom to retrieve the decryption key? |

|  |  |
| --- | --- |
| **Date:**  March 1, 2023 | **Entry:** #2 |
| Description | Analyzing a packet capture file |
| Tool(s) used | Wireshark – to analyze a packet capture file |
| The 5 W's | * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A |
| Additional notes | I was excited to begin to use Wireshark with this exercise and analyze a packet capture file. I can see why it is such a powerful tool for understanding network traffic. |

|  |  |
| --- | --- |
| **Date:**  March 3, 2023 | **Entry:** #3 |
| Description | Capturing my first packet |
| Tool(s) used | Tcpdump – to capture and analyze network traffic |
| The 5 W's | * **Who**: N/A * **What**: N/A * **When**: N/A * **Where**: N/A * **Why**: N/A |
| Additional notes | Using the command-line interface to capture and filter network traffic was a challenge. But after redoing some steps, I was able to get through activities and capture network traffic. |

|  |  |
| --- | --- |
| **Date:**  March 10, 2023 | **Entry:** #4 |
| Description | Investigate a suspicious file hash |
| Tool(s) used | VirusTotal – to investigate and analyze files and URLs for malicious content such as viruses, worms, trojans, and more.  Incident occurred in the Detection and Analysis phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. I had to perform deeper analysis and investigation to determine if the alert signified a real threat. |
| The 5 W's | * **Who**: An unknown malicious actor * **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file has of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b * **When**: At 1:20 p.m. * **Where**: An employee’s computer at a financial services company * **Why**: An employee was able to download and execute a malicious file attachment via e-mail |
| Additional notes | How can the incident be prevented in the future? |

Reflection/Notes:

**1**. **Were there any specific activities that were challenging for you? Why or why not?**

I really found the activity using tcpdump challenging. I am new to using the command line, and learning the syntax for a tool like tcpdump was a big learning curve. At first, I felt very frustrated because I wasn't getting the right output. I redid the activity and figured out where I went wrong. What I learned from this was to carefully read the instructions and work through the process slowly.

**2. Has your understanding of incident detection and response changed after taking this course?**

After taking this course, my understanding of incident detection and response has definitely evolved. At the beginning of the course, I had some basic understanding of what detection and response entailed, but I didn't fully understand the complexity involved. As I progressed through the course, I learned about the lifecycle of an incident; the importance of plans, processes, and people; and tools used. Overall, I feel that my understanding has changed, and I am equipped with more knowledge and understanding about incident detection and response.

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |

|  |  |
| --- | --- |
| **Date:**  Record the date of the journal entry. | **Entry:**  Record the journal entry number. |
| Description | Provide a brief description about the journal entry. |
| Tool(s) used | List any cybersecurity tools that were used. |
| The 5 W's | Capture the 5 W's of an incident.   * **Who** caused the incident? * **What** happened? * **When** did the incident occur? * **Where** did the incident happen? * **Why** did the incident happen? |
| Additional notes | Include any additional thoughts, questions, or findings. |